

MANUAL

FOR

CLASSIFIED INFORMATION SYSTEMS SECURITY



U.S. DEPARTMENT OF ENERGY

Director of Office of Nonproliferation and National Security

Distribution:
All Departmental Elements

Initiated By:
Office of
Safeguards and Security

DRAFT
06-06-97

MANUAL FOR CLASSIFIED INFORMATION SYSTEMS SECURITY

1. **PURPOSE.** This Manual provides requirements and implementation instructions for the graded protection of all classified automated information and special categories of unclassified automated information under the security cognizance of NN, collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the Department of Energy (DOE). The requirements are based upon applicable Federal statutes, regulations, National Security directives, Executive Orders, procedures in Office of Management and Budget Circulars and Bulletins, and Federal standards.
2. **SUMMARY.** All automated information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, DOE requires some level of protection. The loss or compromise of information entrusted to the Department or its contractors may affect the nation's economic competitive position, the environment, the national security, Departmental missions, or the citizens of the United States. The risk management approach defined in this Manual for DOE organizations and DOE contractors provides for the graded, cost-effective protection of classified automated information and special categories of unclassified automated information under the security cognizance of NN.
3. **DEFINITIONS.** See Attachment 1.
4. **CONTACT.** Questions concerning this Manual should be directed to the Classified Information Systems Security Program Manager at 301-903-3019.
5. **CANCELLATIONS.** The Manual DOE M 5639.6A-1 is canceled. Cancellation of a Manual does not, by itself, modify or otherwise affect any contractual obligation to comply with such a Manual. Canceled Manuals incorporated by reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Manuals.
6. **IMPLEMENTATION.** Security requirements for classified information systems contained in this Manual and DOE O 471.2, INFORMATION SECURITY PROGRAM, are to be implemented as follows.
 - a. Existing accredited classified information systems shall remain accredited until reaccreditation is required, either because of expiration of accreditation (3 years) or because of significant changes in the security requirements of the information system. Reaccreditation shall be accomplished under the requirements of this Manual and DOE O 471.2.

DRAFT

- b. Classified information systems that have begun certification and security performance testing on issuance of this manual may be accredited under DOE M 5639.6A-1. These systems shall remain accredited until reaccreditation is required, either because of expiration of accreditation (3 years) or because of significant changes in the security requirements of the information system. Reaccreditation shall be accomplished under the requirements of this Manual and DOE O 471.2.
- c. New classified information systems that are under development and that have not begun certification and security performance testing shall meet the requirements of this Manual and DOE Order 471.2.

DRAFT

CONTENTS

1. PURPOSE	i
2. SUMMARY	i
3. DEFINITIONS	i
4. CONTACT	i
5. CANCELLATIONS	i
6. IMPLEMENTATION	i

CHAPTER I - CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM OVERVIEW

1. INTRODUCTION	I-1
2. MANAGEMENT STRUCTURE	I-1
3. RISK MANAGEMENT	I-1
4. REQUIREMENTS	I-1

CHAPTER II - MANAGEMENT STRUCTURE AND RESPONSIBILITIES

1. CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISPM)	II-1
2. DOE OFFICE MANAGER	II-4
3. DESIGNATED APPROVING AUTHORITY (DAA)	II-4
4. CLASSIFIED INFORMATION SYSTEMS SECURITY OPERATIONS MANAGER(s) (ISOM)	II-5
5. SITE MANAGER(s),	II-5
6. CLASSIFIED INFORMATION SYSTEMS SECURITY SITE MANAGER(s) (ISSM)	II-6
7. CLASSIFIED INFORMATION SYSTEMS SECURITY OFFICER(s) (ISSO)	II-7

CHAPTER III - RISK MANAGEMENT PROCESS

1. INTRODUCTION	III-1
2. THREAT ANALYSIS	III-1
3. DEPARTMENTAL RISK ANALYSIS	III-2
4. DATA OWNER RESPONSIBILITIES	III-2
5. SITE PROGRAM IMPLEMENTATION	III-2
6. NEW OR MODIFIED SYSTEM IMPLEMENTATION	III-2
7. SYSTEM OPERATION	III-2
8. DOE INCIDENT REPORTING	III-2
9. OVERSIGHT	III-3

DRAFT

CHAPTER IV - CERTIFICATION AND ACCREDITATION

CONTENTS (continued)

1. OVERVIEW	IV-1
2. CERTIFICATION PROCESS	IV-1
3. ACCREDITATION.	IV-1
4. DESIGNATED APPROVING AUTHORITY	IV-3
5. ALTERNATIVE PROTECTION MEANS AND DEVIATIONS	IV-3

CHAPTER V - REQUIREMENTS FOR INTERCONNECTED SYSTEMS

1. INTERCONNECTED SYSTEMS MANAGEMENT	V-1
2. CONTROLLED INTERFACE FUNCTIONS	V-2
3. CONTROLLED INTERFACE REQUIREMENTS	V-3
4. ASSURANCES FOR CIs	V-3

CHAPTER VI - PROTECTION PROFILES

1. INTRODUCTION	VI-1
2. LEVELS OF CONCERN	VI-1
3. PROTECTION LEVEL	VI-1
4. CONFIDENTIALITY COMPONENTS	VI-1
5. INTEGRITY COMPONENTS.	VI-1
6. AVAILABILITY COMPONENTS	VI-1
7. COMMON REQUIREMENTS	VI-1
8. GRADED REQUIREMENTS	VI-1
9. EMBEDDED SYSTEMS	VI-2
Table 1. Protection Profile Table for Confidentiality.	VI-3
Table 2. Protection Profile Table for Integrity.	VI-4
Table 3. Protection Profile Table for Availability	VI-4

CHAPTER VII - LEVELS OF CONCERN

1. INFORMATION SENSITIVITY MATRICES	VII-1
2. CONFIDENTIALITY LEVEL OF CONCERN	VII-1
3. INTEGRITY LEVEL OF CONCERN	VII-1
4. AVAILABILITY LEVEL OF CONCERN	VII-1
5. PROTECT AS RESTRICTED DATA (PARD)	VII-2
Table 4. Information Sensitivity Matrix for Confidentiality	VII-4

DRAFT

Table 5. Information Sensitivity Matrix for Integrity	VII-4
Table 6. Information Sensitivity Matrix for Availability.	VII-5

CONTENTS (continued)

CHAPTER VIII - PROTECTION LEVELS

1. INTRODUCTION	VIII-1
2. PROTECTION LEVELS	VIII-1
3. SIGNIFICANT RISK SYSTEMS	VIII-2
4. SUBSTANTIAL RISK SYSTEMS	VIII-2
5. SPECIAL CATEGORIES	VIII-2
Table 7. Protection Level Table for Confidentiality	VIII-6

CHAPTER IX - BASELINE REQUIREMENTS

1. INTRODUCTION	IX-1
2. CLEARING AND SANITIZATION	IX-1
3. EXAMINATION OF HARDWARE AND SOFTWARE	IX-1
4. IDENTIFICATION AND AUTHENTICATION MANAGEMENT	IX-2
5. MAINTENANCE	IX-3
6. MALICIOUS CODE	IX-6
7. MARKING HARDWARE, OUTPUT, AND MEDIA	IX-7
8. PERSONNEL SECURITY	IX-8
9. PHYSICAL SECURITY	IX-11
10. PROTECTION OF MEDIA	IX-11
11. REVIEW OF OUTPUT	IX-12

CHAPTER X - PROTECTION REQUIREMENTS

1. INTRODUCTION	X-1
2. ALTERNATIVE POWER SOURCE	X-1
3. AUDIT CAPABILITY	X-2
4. BACKUP AND RESTORATION OF DATA	X-3
5. CHANGES TO DATA	X-4
6. COMMUNICATIONS	X-5
7. CONFIGURATION MANAGEMENT	X-7
8. DISASTER RECOVERY PLANNING	X-8
9. INDEPENDENT VALIDATION AND VERIFICATION	X-9

DRAFT

10. RESOURCE ACCESS CONTROLS	X-10
11. RESOURCE UTILIZATION	X-11
12. SESSION CONTROLS	X-11
13. SECURITY DOCUMENTATION	X-13
14. SEPARATION OF FUNCTIONS	X-16
15. SYSTEM RECOVERY	X-16

CONTENTS (continued)

16. SECURITY SUPPORT STRUCTURE	X-17
17. SECURITY TESTING	X-18
18. TRUSTED PATH	X-20

ATTACHMENT 1 - DEFINITIONS

DRAFT

CHAPTER I

CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM OVERVIEW

1. **INTRODUCTION.** The Department of Energy (DOE) Classified Information Systems Security Program provides for the protection of classified information and special categories of unclassified information under the security cognizance of NN on DOE and DOE contractor information systems.¹ This program consists of three main elements: Management Structure, Risk Management, and Requirements.
2. **MANAGEMENT STRUCTURE.** Management of the Classified Information Systems Security Program is performed through a multi-tiered structure. DOE Office positions include a Department Classified Information Systems Security Program Manager (ISPM), the Designated Approving Authority (DAA), and the Classified Information Systems Security Operations Manager (ISOM). Site positions include the Classified Information Systems Security Site Manager (ISSM) and the Classified Information Systems Security Officer (ISSO). Details of the management structure and responsibilities are described in Chapter II.
3. **RISK MANAGEMENT.** Risk management is a process that considers the prevailing DOE threat analysis, the effect of countermeasures applied to the processing environment, the remaining vulnerability of the processing environment (residual risk), and the protection requirements and value of the information being processed. Countermeasures are increased until the risk is reduced to an acceptable level or until the cost of reducing the risk becomes prohibitive. If the DAA determines that the remaining risk is not acceptable, management must then determine if the automation requirements are sufficient to justify additional costs. Details of the Risk Management Process are in Chapter III.
4. **REQUIREMENTS.** The Department's classified information systems security process and the baseline requirement for achieving adequate protection based on level of concern for the confidentiality, integrity, and availability of information are detailed in Chapters VI-X. Additional requirements for interconnected systems (networks) are detailed in Chapter V.

¹ In this Manual, the term "system" is used in its general meaning as "Information System or Network." The term is meant to be used so that the distinction between traditional systems and networks is irrelevant to the selection of protection requirements. Special categories of unclassified information under the security cognizance of NN are defined in Attachment 1, page 3.

CHAPTER II

MANAGEMENT STRUCTURE AND RESPONSIBILITIES

Management of the Classified Information Systems Security Program is performed through a multi-tiered structure. The structure includes an ISPM, DAA(s) and ISOM(s) in the DOE Office, and ISSMs and ISSOs at the sites. The following describes the roles and responsibilities of the individuals involved in the decision-making activities in the Program:

1. **CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISPM):**

- a. Is a DOE employee knowledgeable in Information Systems Security appointed by the Director of the Office of Safeguards and Security (NN-51).
- b. Serves as the Program Manager for Classified Information Systems Security, and ensures the implementation of the Classified Information Systems Security Program within the DOE.
- c. Develops and recommends DOE policies, standards, procedures, and guidelines for the protection of information systems that collect, create, process, transfer, store, or provide access to classified information or special categories of unclassified information under the security cognizance of NN.
- d. Maintains a continuing review of this Manual to ensure that current technology is being applied to the protection of information systems that create, process, store, transfer, or provide access to classified information or special categories of unclassified information under the security cognizance of NN and to eliminate those practices that are no longer needed or effective.
- e. Approves secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information.
- f. Annually reviews and updates, as needed, the Periodic Risk Assessment for the U. S. Department of Energy Classified Information Systems Security Program and the DOE Statement of Generic Threat to Automated Information Systems.
- g. Designates the DAA for information systems that involve multiple DAA(s)
- h. Accredits systems operating at a Protection Level of 5 or 6.

DRAFT

- i. Represents the DOE before Federal, private, and public organizations concerned with the protection of classified information systems.
- j. Reports changes in ISOM and DAA appointments to all DAA(s).
- k. Coordinates:
 - (1) with the Unclassified Computer Security Program Manager;
 - (2) with the Office of Energy Intelligence on the protection of Sensitive Compartmented Information;
 - (3) the implementation of the Classified Information Systems Security Program with the Classified Material Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Distribution Systems, TEMPEST, Materials Control and Accountability, and other programs, as appropriate;
 - (4) the development, publishing, and distribution of guidelines for the protection of classified information systems;
- l. Provides education, awareness, and training activities that:
 - (1) Ensure that education in DOE's Classified Information Systems Security policies and practices is available to the ISOMs and ISSMs. The scheduling of these educational activities shall allow all ISOMs and ISSMs to participate within 1 year of their appointment.
 - (2) Maintain a capability to facilitate the electronic exchange of Information Systems Security information, such as awareness alerts on sniffer attacks, viruses, etc.
 - (3) Periodically present Information Systems Security workshops.
 - (4) Periodically sponsor an information systems security program training conference.
 - (5) Ensure that personnel are trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system. This initial training includes the following:
 - threats, vulnerabilities, and risks associated with the information system;

DRAFT

- information and storage media handling, accessibility, and storage considerations;
- system data and access controls; and
- responsibilities associated with the system security.

As a follow-up to this initial training, all individuals who access these systems are required to participate in an ongoing security education, training, and awareness program. Such a program shall ensure that the individuals accessing the information systems are aware of proper operational and security-related procedures and risks. This training and awareness program includes, but is not limited to, various combinations of classes (both self-paced and formal), security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids.

- m. Supports, maintains, and coordinates an advice and assistance capability for use by any ISOM or ISSM within DOE. The services provided by this capability shall include the following:
 - (1) Advice and Assistance Reviews. Reviews of information systems protection as requested by the site, such as reviews of network designs or protection profiles of networks or systems.
 - (2) Independent Validation and Verification. Design, certification, and performance test reviews of networks or systems processing classified information with a Protection Level of 5 or 6.
- n. Maintains and coordinates an incident response capability to provide timely assistance and system vulnerability information to DOE sites.
- o. Provides guidance for a program of technology development to support the DOE Classified Information Systems Security Program, and periodically brief DAAs, ISOMs, and ISSMs on activities and results of the program.
- p. Collects and disseminates information relevant to the Classified Information Systems Security Program.
- q. Monitors the Classified Information Systems Security Program findings and deficiencies resulting from surveys, inspections, and reviews.

DRAFT

- r. Conducts timely review of the protection documentation for information systems located in Sensitive Compartmented Information Facilities that process, store, transfer, or provide access to intelligence information.
- s. Reviews certification of the information system located in Sensitive Compartmented Information Facilities received from cognizant ISOM(s) and provides comments to the Office of Energy Intelligence.

2. DOE OFFICE MANAGER:

- a. Appoints, in writing, a DOE employee to serve as the DAA for information systems under his/her cognizance and notifies the ISPM of this appointment. (The same person may be appointed as both the DAA and ISOM.)
- b. Appoints, in writing, one or more DOE employee(s) knowledgeable in information systems security as the ISOM(s) for classified information systems under the cognizance of the DOE Office and notifies the ISPM of this appointment.
- c. Ensures:
 - (1) the implementation of this Manual for information systems under his/her management and control, including those of contractors under the cognizance of the DOE Office; and
 - (2) that the ISOM(s) and all ISSM(s) at sites under his/her jurisdiction receive ISPM-sponsored training in the DOE Classified Information Systems Security Program within 1 year of appointment.

3. DESIGNATED APPROVING AUTHORITY (DAA). The DAA shall be responsible for evaluating the protection measures in a system as described in the Systems Security Plan (SSP), the results of any certification tests, the certification of the system, and any residual risks of operating the system. Accordingly, the DAA:

- a. Has written authorization to accept the residual risk and responsibility for the loss of confidentiality, availability, and/or integrity of all classified information systems under his/her jurisdiction. The authorization shall include provisional accreditation, withdrawal of accreditation, and suspension of operations for all classified information systems under his/her jurisdiction.

DRAFT

- b. Serves as accrediting authority for each DOE and covered contractor classified information system operating at a Protection Level of 1-4.
 - c. Ensures each classified information system under his/her jurisdiction is accredited or reaccredited at least every 3 years (except for information systems processing Sensitive Compartmented Information) and that the accreditation or reaccreditation is documented.
 - d. Ensures DAA authorities are delegated to DOE employees who are knowledgeable individuals.
 - e. Reports any changes in ISOM or ISSM appointments to the ISPM.
4. CLASSIFIED INFORMATION SYSTEMS SECURITY OPERATIONS MANAGER(s) (ISOM):
- a. Communicates incident reports received from sites to the ISPM.
 - b. Ensures the regular review of the Classified Information Systems Security Program at each site under the jurisdiction of the DOE Office.
 - c. Evaluates information systems for accreditation when requested by the DAA.
 - d. Monitors the responses to findings and other deficiencies identified in surveys, inspections, and reviews of each site Classified Information Systems Security Program to ensure that any necessary corrective or compensatory actions have been completed.
 - e. Coordinates:
 - (1) the Classified Information Systems Security Program with the unclassified information systems security program and
 - (2) the implementation of the Classified Information Systems Security Program with the Classified Material Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Distribution Systems, TEMPEST, Materials Control and Accountability, and other programs, as appropriate.
5. SITE MANAGER(s), where information systems are operated, shall ensure:
- a. the implementation of a Classified Information Systems Security Program;

DRAFT

- b. that managers and supervisors are aware of, and fulfill, their responsibilities for the protection of classified information;
- c. the identification and funding of the independent validation and verification of classified information systems with a Protection Level of 5 or 6;
- d. the appointment, in writing, of an ISSM who is responsible for the implementation of the site Classified Information Systems Security Program; a separate ISSM may be appointed for information systems in a Sensitive Compartmented Information Facility if the site determines that another ISSM is needed;
- e. that the ISSM(s) under his/her jurisdiction participate in ISPM-sponsored information systems security education within 1 year of appointment.
- f. that he/she reports any changes in ISSM appointments to the cognizant DAA(s).

6. CLASSIFIED INFORMATION SYSTEMS SECURITY SITE MANAGER(s) (ISSM):

- a. Acts as the site point of contact for all classified information systems security activities, including inspections, tests, and reviews.
- b. Ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data owners, and users.
- c. Ensures the development, documentation, and presentation of information systems security training for escorts for information systems.
- d. Establishes, documents, implements, and monitors the Classified Information Systems Security Program for the site and ensures site compliance with DOE policies, standards, and procedures for information systems.
- e. Ensures the development of procedures for use in the site's classified information systems security program.
- f. Identifies and documents unique threats to information systems at the site.
- g. Ensures that the site's Classified Information Systems Security Program is coordinated with the Site Safeguards and Security Plan or the Site Security Plan.

DRAFT

h. Coordinates:

- (1) implementation of the site Classified Information Systems Security Program with the Classified Material Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Distribution Systems, TEMPEST, Materials Control and Accountability, and other site programs, as appropriate;
 - (2) development of a site self-assessment program for the Classified Information Systems Security Program;
 - (3) performance of a self-assessment of the site Classified Information Systems Security Program, between surveys.
- i. Ensures the development, in coordination with the Classified Matter Protection and Control Operations Manager, of site procedures to govern marking, handling, controlling, removing, transporting, sanitizing, reuse, and destruction of media and equipment containing classified information.

7. CLASSIFIED INFORMATION SYSTEMS SECURITY OFFICER(s) (ISSO):

- a. Ensures the implementation of security measures for each classified information system for which he/she is responsible.
- b. Prepares, maintains, and implements a Classified Systems Security Plan (SSP) that accurately reflects the installation and security provisions for each classified AIS for which he/she is responsible.
- c. Identifies and documents any unique threats for the classified information systems for which he/she is the ISSO and forwards them to the ISSM.
- d. Performs a risk assessment to determine if additional countermeasures beyond those identified in this Manual are required, if so directed by the DAA and/or an identified unique local threat exists.
- e. Develops and implements a certification test plan for each classified information system operating at a Protection Level of 4, 5, or 6 for which he/she is the ISSO.
- f. Advises the ISSM, in writing, that the Classified Information Systems Security Program has been implemented as described in the SSP and that the specified security controls are in place and properly implemented.

DRAFT

- g. Maintains the record copy of the SSP and related documentation for each classified Information System for which he/she is the ISSO.
- h. Ensures:
 - (1) the development, documentation, and testing, if required, of a continuity of operations plan based on guidance from the responsible management official;
 - (2) that each classified information system for which he/she is responsible is covered by the site Configuration Management Program;
 - (3) that the proper sensitivity level of the information is determined prior to use on the Classified Information System and that the proper security measures are implemented to protect this information;
 - (4) that unauthorized personnel are not granted use of, or access to, a classified information system;
 - (5) the implementation of formal access controls for each classified information system, except personal computers and stand-alone workstations.
- i. Documents any special security requirement identified by the data owners and the protection measures implemented to fulfill these requirements for the information contained in the classified information system.
- j. Implements site procedures:
 - (1) in coordination with the Classified Matter Protection and Control Operations Manager, to govern marking, handling, controlling, removing, transporting, sanitizing, reuse, and destruction of media and equipment containing classified information;
 - (2) to ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented;
 - (3) for the reporting of classified information systems security incidents;
 - (4) requiring that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for the security of classified information systems and classified information;

DRAFT

- (5) for the detection of malicious code, viruses, and intruders (hackers).
- k. Identifies classified Information Systems Security training needs (including system-specific training) to ensure that system users are properly trained and recommends personnel to attend training programs.
- l. Conducts classified information systems ongoing security reviews and testing to periodically verify that security features and operating controls are functional and effective.
- m. Evaluates proposed changes or additions to the classified information systems and advises the ISSM of their security relevance.

CHAPTER III

RISK MANAGEMENT PROCESS

1. **INTRODUCTION.** The cornerstone of DOE's Classified Information Systems Security Program is the risk management process, which determines the protection requirements for DOE's information. Risk management balances the data owner's perceived value of the information and the data owner's assessment of the consequences of loss of confidentiality, integrity, and availability against the costs of protective countermeasures and day-to-day operations. DOE's risk management process includes the following interrelated phases:
 - a. threat analysis;
 - b. Departmental risk analysis where the generic threats, technologies, and architectures are evaluated and integrated into DOE policies, guidelines, and standards;
 - c. data owner declaration of the consequences of loss of confidentiality, integrity, and availability;
 - d. site program implementation where the unique concerns of the site (i.e., threats, protective technologies, procedures, etc.) are evaluated and integrated with site operations;
 - e. system implementation where the impact of information loss, system vulnerabilities, data owner protection requirements, cost of protective measures, and mission requirements are identified, evaluated, and integrated;
 - f. system operation where the remaining risk (residual risk) is accepted and oversight is initiated to ensure that the level of residual risk is managed throughout the information system's life cycle; and
 - g. oversight activities that support and improve the risk management approach through reviews of the classified information systems security program implementation in the DOE Offices and sites.
2. **THREAT ANALYSIS.** The analysis of information threats identified by national and DOE organizations provides the basis for protecting DOE's classified information and special categories of unclassified information under the security cognizance of NN. The ISPM shall annually review the Nation's information threat posture. The results of this review shall be

DRAFT

used to develop or update the DOE Statement of Generic Threat to Automated Information Systems.

3. DEPARTMENTAL RISK ANALYSIS. This process begins with an analysis of information architectures and technologies to determine how information with different sensitivities can be protected on an information system. A risk assessment is then performed using this analysis and the DOE Statement of Generic Threat to Automated Information Systems. The results of this risk assessment are used as the basis to develop the protection countermeasures for DOE's information.
 - a. DOE Risk Assessment. The ISPM shall maintain a constant awareness of technology, technology trends, information architectures, and information standards as they relate to protecting information. This information, and the DOE Statement of Generic Threat to Automated Information Systems, shall be used by the ISPM to perform the Periodic Risk Assessment for the U. S. Department of Energy Classified Information Systems Security Program.
 - b. Changes to Policy and Guidelines. If either the DOE Statement of Generic Threat to Automated Information Systems or the Periodic Risk Assessment for the U. S. Department of Energy Classified Information Systems Security Program is changed, the ISPM shall conduct an analysis to identify and recommend changes to DOE requirements in DOE O 471.2 and this Manual.
4. DATA OWNER RESPONSIBILITIES. The owner of each piece of information collected, created, processed, transmitted, or stored on an automated information system is expected to declare the level of sensitivity or classification of information on the automated system.
5. SITE PROGRAM IMPLEMENTATION. The Periodic Risk Assessment for the U. S. Department of Energy Classified Information Systems Security Program and any site-specific threats shall be incorporated into a site risk assessment. The site risk assessment shall consider any protection technologies unique to the site, the cost of protection measures, the information protection requirements, and the impact of protection measures on the information system mission. The results of the site risk assessment shall be used to define the classified information systems protection profiles to be applied to information systems at the site. The results of the risk assessment shall be documented.
6. NEW OR MODIFIED SYSTEM IMPLEMENTATION. The system implementation process begins with identifying the level of concern and protection level of the information to be processed. The protection profile is determined based on the levels of concern and

DRAFT

protection level. The protection profile requirements are then integrated into the information systems design, implementation, and operation.

7. SYSTEM OPERATION. The final phase of the risk management process is the acceptance of risk through certification and accreditation, and the protection of information during day-to-day operations.
8. DOE INCIDENT REPORTING. In addition to the reporting requirements of DOE O 232.1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS
9. OVERSIGHT.
 - a. ISOM Program Reviews. The ISOM shall ensure that periodic reviews of the site's Classified Information Systems Security Program are performed.
 - b. ISSM Self Assessments. The ISSM shall ensure that periodic assessments of the site's program are performed. Upon completion of each review, the ISSM shall ensure the preparation and implementation of a corrective action plan for all identified findings or vulnerabilities as directed by DOE Order 470.1, Chapter IX, Paragraph 10a. A record of each review and the subsequent corrective action plan shall be maintained and available for future surveys and inspections.

CHAPTER IV

CERTIFICATION AND ACCREDITATION

1. OVERVIEW. The certification and accreditation process begins after the protection measures have been implemented on a system and any required information systems protection documentation has been approved. The certification process validates that a protection profile has been selected, that the protection profile has been implemented on the system, and that the protection measures are functioning properly. This process culminates in an accreditation for the system to operate.
2. CERTIFICATION PROCESS. The certification process subjects the system to appropriate verification that it has been implemented in accordance with the selected protection profile and validates that each required protection measure has been implemented.
 - a. Independent Validation and Verification. For information systems intended to operate in Protection Levels 5 and 6, an Independent Validation and Verification (IV&V) review shall support the certification process.
 - b. Sensitive Compartmented Information. For information systems located in a Sensitive Compartmented Information Facility that processes sensitive compartmented information, the cognizant ISSM, ISOM, and ISPM shall review the information system protection documentation and the certification of the information system and direct it, with their comments, to the Office of Energy Intelligence, Office of Nonproliferation and National Security.
3. ACCREDITATION. All systems shall be reviewed and accredited to operate by the DAA.
 - a. Provisional Accreditation. The DAA may grant provisional accreditation (temporary authority) to operate an information system because of incomplete documentation, or to permit a major conversion of the information system. This provisional accreditation may be granted for up to 180 days. DAA-approved protection measures shall be in place and functioning during the period of provisional accreditation.
 - b. Reaccreditation. Following the intent of OMB Circular A-130, "Management of Federal Information Resources," each information system shall be reaccredited every 3 years at a minimum. Information system accreditation shall be reviewed immediately if modifications to the information system impact its protection, if the protection aspects of its environment change, or if the applicable protection requirements change.

DRAFT

- c. Withdrawal of Accreditation. The DAA shall evaluate the risks and consider withdrawal of accreditation if the protection measures and controls approved for the system do not remain effective or whenever any of the following change: levels of concern, protection level, technical or nontechnical security safeguards, vulnerabilities, operational environment, operational concept, or interconnections.
- d. Certification and Accreditation of Multiple Systems. If two or more similar information systems are to be operated in equivalent operational environments (i.e., the levels of concern and protection level are the same and the physical security requirements are similar), a Master Systems Security Plan (SSP) may be written and approved by the DAA to cover all such information systems. The information systems covered by a Master SSP may range from personal computers up to and including multiuser information systems and local area networks that meet the criteria for a master plan approach.
- (1) Master Systems Security Plan. The Master SSP for these information systems shall specify the information required for each certification for an information system to be accredited under the plan.
 - (2) Information Systems Documentation. The ISSM shall ensure that each information system covered by a Master SSP is documented with:
 - the information system identification,
 - the information system location,
 - the Master SSP covering the information system, and
 - a statement signed by the ISSO certifying that the information system implements the requirements in the Master SSP.
 - (3) Information Systems Accreditation. The DAA shall accredit the first information system under the Master SSP. All other individual information systems to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP. This certification, in effect, accredits the individual information systems to operate under the Master SSP. A copy of each certification report shall be retained with the approved copy of the Master SSP.
 - (4) Recertification of Information Systems. All information systems certified under a Master SSP remain certified until the Master SSP is changed or 3 years have

DRAFT

elapsed since the information system was certified. If the level of concern or protection level described in the Master SSP changes, all information systems certified under the Master SSP shall be re-certified.

4. DESIGNATED APPROVING AUTHORITY.

- a. Systems at Protection Levels 5 and 6. The ISPM shall be the DAA for systems at Protection Levels 5 and 6.
 - b. Delegation of Approval Authority. The DAA may delegate approval authority. Rules for this delegation are that:
 - (1) all delegations shall be in writing and for a specified time period not to exceed 3 years;
 - (2) the DAA (or his/her delegate) and the person certifying the system shall not be the same person;
 - (3) the delegate cannot redelegate the approval authority; and
 - (4) the delegate must be a federal employee.
 - c. Systems under Multiple Approving Authorities. For systems that involve multiple DAAs, the ISPM shall serve as or select the approving authority. Each site involved in the system shall identify, in writing, the security officials to be responsible for implementing information system protection on the system components at the site.
 - d. Director of Naval Reactors Program. For information systems networks that are solely under the jurisdiction of the Director of Naval Reactors Program and whose external components extend into the jurisdiction of different Naval Reactor Offices, the Director of Naval Reactors Program shall designate one of the Naval Reactor Office senior managers to be the DAA. Notification of the accreditation of any information system with a Protection Level of 4, 5, or 6 shall be furnished to the ISPM.
5. ALTERNATIVE PROTECTION MEANS AND DEVIATIONS. If it is impossible or impracticable to implement the protection requirements and countermeasures described in this Manual in the classified information system, alternative protection means and deviations (variances, waivers, or exceptions) shall be approved under the procedures described in DOE O 470.1.

DRAFT

CHAPTER V

REQUIREMENTS FOR INTERCONNECTED SYSTEMS

1. INTERCONNECTED SYSTEMS MANAGEMENT. The characteristics and capabilities of classified systems implemented as networks require special security considerations. This chapter **imposes additional requirements** on a network or expands on the security requirements stated in Chapters IX and X as they apply to a network.
 - a. When connecting two or more networks, the DAA(s) shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.
 - b. A unified network is a connected collection of systems or networks that are accredited **(1) under a single SSP, (2) as a single entity, and (3) by a single DAA**. Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single DAA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.
 - c. An **interconnected** network is comprised of **two or more separately accredited systems and/or networks**. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a Security Support Structure (SSS) capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.
 - d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:
 - (1) they are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or

DRAFT

- (2) both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or
 - (3) both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.
- e. Any classified system connected to another system that does not meet either (2) or (3) above shall utilize a Controlled Interface(s) (CI) that performs the following.
 - (1) A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.
 - (2) A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.
 - (3) Communications from outside the system perimeter shall have an authorized user as the destination (i.e., the CI shall notify the user of the communication and release the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

2. CONTROLLED INTERFACE FUNCTIONS.

- a. The functions of the CI include:
 - (1) providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts;
 - (2) providing a reliable exchange of security-related information; or
 - (3) filtering information in a data stream based on associated security labels for data content.
- b. CIs have several characteristics including the following.
 - (1) There are NO GENERAL USERS on the CI.
 - (2) There is NO USER CODE running on the CI.

DRAFT

- (3) The CI provides a protected conduit for the transfer of user data.
 - (4) Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.
3. CONTROLLED INTERFACE REQUIREMENTS. The CI shall have the following properties.
- a. Adjudicated Differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.
 - b. Routing Decisions. The CI shall base its routing decisions on information that is supplied or alterable only by the SSS.
 - c. Restrictive Protection Requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or information systems.
 - d. User Code. The CI shall not run any user code.
 - e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.
 - f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.
 - g. Technical Protection Requirements. The platform on which the CI is operating usually need meet no more than the technical protection requirements for Protection Level 3. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) are protected from unauthorized access or circumvention from other applications or users.

4. ASSURANCES FOR CIs. Each CI shall be tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation, alone.

CHAPTER VI

PROTECTION PROFILES

1. **INTRODUCTION.** A protection profile (PP) describes the protection measures that must be addressed throughout the system lifecycle. PPs are used to organize protection measures into a set of requirements. The requirements are graded, based on the levels of concern and protection level, and include any information protection requirements defined by the data owner. The PP for a specific information system is based on the information levels of concern and the protection level. A PP contains (1) a description or definition of the system environment, (2) the confidentiality measures, (3) the integrity measures, and (4) the availability measures.
2. **LEVELS OF CONCERN.** The level of concern reflects the data owner's perceived value of the information and the consequences of the loss of integrity, availability, or confidentiality. If the data owner has not established the level of concern, the data steward, with the assistance of the ISSO, will do so. The levels of concern are listed in Chapter VII.
3. **PROTECTION LEVEL.** The protection level describes the information system's user community. The protection levels are based on the users' need-to-know, formal access approval(s), and access authorizations (clearances). These protection levels are defined in Chapter VIII.
4. **CONFIDENTIALITY COMPONENTS.** Confidentiality components describe the confidentiality protection requirements that must be implemented in an information system using the profile. The confidentiality protection requirements shall be graded according to the confidentiality protection levels that incorporate levels of concern.
5. **INTEGRITY COMPONENTS.** Integrity components describe the integrity protection requirements that must be implemented in an information system using the profile. The integrity protection requirements shall be graded according to the integrity levels of concern.
6. **AVAILABILITY COMPONENTS.** Availability Components describe the availability protection requirements that must be implemented in an information system using the profile. The availability protection requirements shall be graded according to the availability levels of concern.
7. **COMMON REQUIREMENTS.** Requirements common to all systems are detailed in Chapter IX - Baseline Requirements.

DRAFT

8. GRADED REQUIREMENTS. Requirements graded by level of concern and confidentiality protection level are detailed in Chapter X - Protection Requirements. The following tables present the requirements detailed in Chapter X - Protection Requirements. To use these tables, find the column representing the protection level for confidentiality, or find the column representing the level of concern for integrity and availability.
9. EMBEDDED SYSTEMS. Some systems cannot be altered without special hardware or software not generally available to users, and are designed and implemented to provide a very limited set of predetermined functions. Certain “embedded” systems fall in this category. If the DAA concurs that such a system is sufficiently incapable of alteration, and that the system provides an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this Manual. DAA, DAA designees, and implementors are cautioned to be sure that such systems, in all operational situations, provide the separation appropriate to the system’s protection level.

Table 1. Protection Profile Table for Confidentiality.

Requirements (Page)						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Audit Capability (X-2)	AUD-1	AUD-1	AUD-2	AUD-3	AUD-4	AUD-4
Communications (X-5)	COM-1	COM-1	COM-1	COM-2	COM-1	COM-1
Configuration Management (X-7)	CM-1	CM-1	CM-1	CM-2	CM-3	CM-3
Independent Validation and Verification (X-9)					IVV-1	IVV-1
Resource Access Control (X-10)		RAC-1	RAC-1	RAC-2	RAC-3	RAC-3
Resource Utilization (X-11)		RU-1	RU-1	RU-2	RU-2	RU-2
Session Controls (X-12)	SC-1	SC-2	SC-2	SC-3	SC-3	SC-3
Security Documentation (X-13)	SD-1	SD-1	SD-2	SD-2	SD-3	SD-3
Separation of Functions (X-16)				SF-1	SF-1	SF-1
System Recovery (X-16)	SR-1	SR-1	SR-1	SR-1	SR-2	SR-2
Security Support Structure (X-17)	SSS-1	SSS-1	SSS-1	SSS-2	SSS-3	SSS-3
Security Testing (X-18)	ST-1	ST-2	ST-2	ST-3	ST-4	ST-4
Trusted Path (X-20)					TP-1	TP-1

DRAFT

Table 2 . Protection Profile Table for Integrity.

Requirements (Page)			
Integrity	Low	Medium	High
Audit Capability (X-1)	AUD-1	AUD-2	AUD-4
Backup and Restoration of Data (X-3)	BRD-1	BRD-2	BRD-3
Changes to Data (X-4)	CD-1	CD-2	CD-3
Communications (X-5)	COM-1	COM-1	COM-2
Configuration Management (X-7)	CM-1	CM-2	CM-3
Security Support Structure (X-17)	SSS-1	SSS-2	SSS-3
Security Testing (X-18)	ST-1	ST-3	ST-4

Table 3. Protection Profile Table for Availability.

Requirements (Page)			
Availability	Low	Medium	High
Alternative Power Source (X-1)	APS-1	APS-2	APS-3
Disaster Recovery Planning (X-8)	DRP-1	DRP-2	DRP-3
Security Support Structure (X-17)	SSS-1	SSS-2	SSS-3

DRAFT

CHAPTER VII

LEVELS OF CONCERN

1. INFORMATION SENSITIVITY MATRICES. The tables in this chapter are designed to assist those involved in system development, implementation, certification, and accreditation in determining the appropriate level of concern for confidentiality, integrity, and availability for a given system processing a given set of information. General guidelines on how to use the Information Sensitivity Matrix include the following.
 - a. A determination of high, medium, or low shall be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.
 - b. When a given system contains more than one kind of information, the level of concern for the system is the highest of the levels of concern for each of the kinds of information.
 - c. The information sensitivity matrices were constructed to assist the DAA in considering the sensitivity of the information and in selecting the level of concern for confidentiality, integrity, and availability. The DAA shall use guidance from the data owner(s) in making this decision.
 - d. The DAA or the data owner may choose to apply a higher level of concern for any aspect of any information on the system.
2. CONFIDENTIALITY LEVEL OF CONCERN. In considering confidentiality, the principal question is the necessity for maintaining the classification levels and the types of information (e.g., SRD Sigma 15) on the system in question. The protection level table for confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a set of graded requirements to protect the confidentiality of the information on the system. This graded approach to risk provides sufficient and necessary protection for the information on the system without requiring unnecessary protections for systems where the level of concern for confidentiality is low or medium.
3. INTEGRITY LEVEL OF CONCERN. In considering integrity, the principal question is the necessity for maintaining the integrity of the information on the system in question. (See Table 5.)

DRAFT

4. AVAILABILITY LEVEL OF CONCERN. In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission. (See Table 6.)
5. PROTECT AS RESTRICTED DATA (PARD).
 - a. Site authorization to use PARD designation. Any site wishing to use the PARD designation must receive the prior approval of the Director, Office of Nonproliferation and National Security (NN-1). The CSOM may limit the use of the PARD designation to specific organizations at a site. Use of the PARD designator will be discontinued permanently on June 30, 2002.
 - b. Handling and control of PARD information.
 - (1) The security measures contained herein apply only to PARD information as it appears as output, hereafter referred to as "PARD output." Only printed computer output may be marked PARD. Electronic media (disks, tapes, etc.) and computer systems may not be marked PARD. Within the classified AIS (including communication lines), information that will be labeled PARD when it is in printed form is Secret-Restricted Data. PARD output may only be generated on AISs that have been accredited to process information at the High Level of Concern for Confidentiality. PARD output may only be used in a DOE Limited or Exclusion security area. PARD output may only be viewed by Q cleared personnel with a need-to-know for the information.
 - (2) Appropriately trained users (see c. below) may determine the use of the PARD marking for their information. The PARD marking shall only be used if the output that is generated may contain limited quantities of classified information that is not readily recognized as classified due to its being contained in large quantities of unclassified information, and the PARD output contains a substantial volume of data with a low density of potentially classified information.
 - (3) PARD output shall be conspicuously marked on each page or sheet with the words "PROTECT AS RESTRICTED DATA." Where space does not allow, the letters "PARD" may be used. This marking shall be applied at the time of origination of the PARD output. All PARD output shall show the date of origination.
 - (4) When not in use, PARD output shall be stored within a Limited or Exclusion security area in a manner authorized for Secret-Restricted Data documents (DOE

DRAFT

471.2, INFORMATION SECURITY PROGRAM); or in a secure storage container or filing cabinet equipped with a locking device; or in an area that is administratively controlled during work hours and maintained under locked conditions during non work hours. The keys/combinations for any locks used to protect PARD must be administratively controlled and only available to persons with at least a Q clearance and a need-to-know for the information.

- (5) PARD output shall be destroyed in the same manner as Secret-Restricted Data documents. Physical destruction shall be accomplished in compliance with DOE 471.2, INFORMATION SECURITY PROGRAM.
- (6) PARD output to be transferred from the site in which it was originated to another site shall be reviewed for classification (DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION) and, if classified, must be marked, handled, protected, and transferred as any other classified document (DOE 471.2/DOE M 471.2, INFORMATION SECURITY PROGRAM). PARD output transferred between points within a Limited or Exclusion security area or between Limited or Exclusion security areas located at the same site shall be in the personal custody of a Q cleared person. Between Limited or Exclusion security areas, the PARD output shall be protected as a Secret-Restricted Data document as specified in DOE 471.2/ DOE M 471.2, INFORMATION SECURITY PROGRAM.

c. Training of PARD users.

The Classified Matter Protection and Control (CMPC) Manager at a site approved for the use of PARD output shall ensure proper control and use of PARD output by ensuring that each user is aware of the special security measures necessary for the handling of PARD output. No user shall be allowed to use the PARD designation until he/she has received appropriate training as specified by the CMPC Manager. The CMPC Manager shall ensure that periodic reviews are conducted to assure that accumulation of PARD output is kept to a minimum and that the PARD marking is being used in compliance with this policy.

DRAFT

Table 4. Information Sensitivity Matrix for Confidentiality.

Level of Concern	Qualifiers
High	All Sensitive Compartmented Information All SAPs All Information Protecting Intelligence Sources, Methods and Analytical Procedures All SIOP All Crypto SECRET RD (SIGMAs 1,2,14,15) TOP SECRET
Medium	SECRET SECRET RD (All other SIGMAs)
Low	CONFIDENTIAL Special Categories of Unclassified Information Under the Security Cognizance of NN

NOTE: The data owner may specify a level of concern that exceeds what is warranted by the table.

Table 5. Information Sensitivity Matrix for Integrity.

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Low	Reasonable degree of accuracy required for mission accomplishment; or loss of integrity will have an adverse effect.

DRAFT

Table 6. Information Sensitivity Matrix for Availability.

Level of Concern	Indicators
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Low	Information must be available with flexible tolerance for delay; or loss of availability will have an adverse effect.

NOTE: In this context, “High - No tolerance for delay” means no delay; “Medium - minimum tolerance for delay” means a delay of seconds to minutes; and “Low - flexible tolerance for delay” means a delay of days to weeks.

DRAFT

CHAPTER VIII

PROTECTION LEVELS

1. INTRODUCTION. The protection level is determined by the relationship between two sets of facts: first, the clearance(s), formal access approval(s), and need-to-know of users; and second, the classification, formal access requirements, and sensitivity of the information on the system. The protection level indicates an implicit level of trust that is placed in the system's technical capabilities.
2. PROTECTION LEVELS. The table at the end of this chapter presents the criteria for determining the following six protection levels for confidentiality:
 - a. Systems are operating at Protection Level 1 when **all** users have all required approvals for access to all information on the system. For systems processing classified information, this means that all users have all required clearance(s), formal access approval(s), and the need to know for all information on the system.
 - b. Systems are operating at Protection Level 2 when **all** users have all required **formal** approval(s) for access to all information on the system, but at least one user lacks administrative approval(s) for some of the information on the system. For systems processing classified information, this means that all users have all required clearance(s) and all required formal access approval(s), but at least one user lacks the need to know for some of the information on the system and **no information on the system has a classification level higher than Confidential** (i.e., the level of concern for confidentiality is low).
 - c. Systems are operating at Protection Level 3 when **all** users have all required **formal** approval(s) for access to all information on the system, but at least one user lacks administrative approval(s) for some of the information on the system. For systems processing classified information, this means that all users have all required clearance(s) and all required formal access approval(s), but at least one user lacks the need to know for some of the information on the system **and the information on the system is at a higher level than Confidential** (i.e., the level of concern for confidentiality is medium or high).
 - d. Systems operating at Protection Level 4 can be of two different kinds. A system must meet the requirements for Protection Level 4 when either of the two following situations exists:

DRAFT

- (1) At least one user lacks at least one required **formal** approval for access to all information on the system. For systems processing classified information, this means that all users have all required clearance(s), but at least one user lacks formal access approval(s) for some of the information on the system.
 - (2) At least one user on the system lacks any sort of clearance and the information on the system is classified no higher than Confidential.
- e. Systems are operating at Protection Level 5 when at least one user has no clearance and the information on the system is classified no higher than Secret and contains no Sigma 1, 2, 14, or 15 (i.e., the level of concern for confidentiality is medium).
- f. Systems are operating at Protection Level 6 when at least one user has no clearance or at least one user is cleared to a level less than Top Secret and the level of concern for confidentiality is high.
3. **SIGNIFICANT RISK SYSTEMS.** Systems operating at Protection Levels 5 and 6 present a **significant** risk of the loss of classified information. Systems operating at Protection Level 5 or 6 are not permitted to have unclassified access from a public switched network (i.e. Internet). Systems operating at these levels may operate within a protected environment or have connections that provide for encrypted data to pass over public switched networks. Any connection of these systems to other agencies will require a memorandum of understanding stating that the system/network being connected is not connected to a system or network with public switched network access capabilities.
4. **SUBSTANTIAL RISK SYSTEMS.** Systems operating at Protection Level 4 present a **substantial** risk of the loss of the separation and need-to-know protection provided by compartmentation. DAAs shall recognize the technical risk of operating such systems.
5. **SPECIAL CATEGORIES.** Several categories of systems can be adequately secured without implementation of all the technical features specified in Chapter X. These systems are **not** “exceptions” or “special cases” of the protection levels specified in this chapter. However, applying the technical security requirements specified in Chapter X to these systems by rote results in unnecessary costs and operational impacts. In general, the technical question is where, when, and how to apply a given set of safeguards, rather than whether to apply the safeguards. For many of these “special” systems (such as guards, pure servers, tactical, data-acquisition, and embedded systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

DRAFT

a. Pure Servers.

- (1) Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the characteristics listed below.
 - (a) No user code is present on the system.
 - (b) Only system administrators and maintainers can access the system.
 - (c) The system provides non-interactive services to clients (e.g., packet routing or messaging services).
 - (d) The hardware and/or application providing network services otherwise meets the security requirements of the network.
 - (e) The risk of attack against the SSS using network communication paths is sufficiently low.
 - (f) The risk of attack against the SSS using physical access to the system itself is sufficiently low.
- (2) The **platform (i.e., hardware and operating system)** on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e., individuals who use the guard's or server's functional capabilities in a severely constrained way). The guard **application** or server **application** itself will have to provide the more stringent technical protections appropriate for the system's protection level and operational environment. Assurances appropriate to the level of concern for the system shall be implemented.
- (3) Systems that **do have general users or do execute general user code** are not "pure servers" within the meaning of this section, and so must meet all security requirements specified for their protection level and operational environment.
- (4) The term "pure server" is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this document and, if such a system

DRAFT

meets the specifications in 5a, above, the system's technical requirements could be categorized by this section.

- (5) The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements), which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines.
- b. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems. Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that: first, and most importantly, there are NO GENERAL USERS on the system; and, second, there is NO USER CODE running on the system. If the DAA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this document. DAAs and implementors are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.
 - c. Systems with Group Authenticators.
 - (1) Many security measures specified in this document implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/authenticator combination. Such situations are often referred to as requiring the use of group authenticators.
 - (2) In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators are used for broader access **after** the use of a unique authenticator for initial identification and authentication.

DRAFT

- d. Single-user, Stand-alone Systems. Extensive technical safeguards are normally inappropriate and inordinately expensive for single-user, stand-alone systems. DAAs can approve administrative and environmental protections for such systems, in lieu of technical safeguards. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the DAA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, and sanitized between users, are periods processing systems as described below.
- e. Periods Processing. Periods processing is a method of sequential operation of an information system that provides the capability to process various levels of sensitivity of information at distinctly different times. Periods processing provides the capability to either:
- have more than one user (sequentially) on a single-user information system with different levels of information or need-to-know;
 - use an information system at more than one protection level (sequentially); or
 - use an information system in more than one protection level at the same time.
- (1) Sanitization After Use. If an information system is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the SSP shall specify the sanitization procedures to be employed by each user before and after each session of use of the system.
- (2) Sanitization Between Periods. The information system shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have security clearance or the need-to-know for data processed during the previous period, changing from one protection level to another). These procedures shall be documented in the SSP and approved by the DAA. Such procedures could include, among others, sanitizing nonvolatile storage, exchanging disks, and powering down the information system and its peripherals.
- (3) Media For Each Period. Information systems employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

- (4) Audit. If there are multiple users of the system and the system is not capable of automated logging, manual logging shall be done at the discretion of the DAA. Audit trails are not required for single-user stand-alone systems.

Table 7. Protection Level Table for Confidentiality.

Level of Concern	Lowest Clearance	Formal Access Approval	Need To Know	Protection Level
High	Uncleared or less than Top Secret	NOT ALL Users Have ALL	NOT ALL Users Have ALL	6
Medium	Uncleared	NOT ALL Users Have ALL	NOT ALL Users Have ALL	5
Low	Uncleared	NOT ALL Users Have ALL	NOT ALL Users Have ALL	4
High, Medium, or Low	At Least Equal to Highest Data	NOT ALL Users Have ALL	NOT ALL Users Have ALL	4
High or Medium	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	3
Low	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Low	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

DRAFT

CHAPTER IX

BASELINE REQUIREMENTS

1. INTRODUCTION. This chapter describes the implementation requirements that are common to all systems.
2. CLEARING AND SANITIZATION.
 - a. Clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information. Detailed instructions on clearing shall be issued periodically by the ISPM.
 - b. Sanitization. Sanitization of a classified AIS resource shall be accomplished before it may be released from classified information controls or released for use at a lower classification level. To sanitize storage media, memory, and hardware, the guidance issued periodically by the ISPM shall be followed.
 - c. Visual Examination of Hardware Components. To complete sanitization of a Classified AIS, any classified media, such as diskettes, disk cartridges, disks, tapes, printer ribbons, and hard copy output, shall be physically removed. An examination of the display device for evidence of residual information shall be conducted.
3. EXAMINATION OF HARDWARE AND SOFTWARE. Information Systems hardware and software shall be examined when received from the vendor and before being placed into use.
 - a. Information Systems Software. Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the information system. Security related software shall be tested to ensure that the security features function as specified.
 - b. Information Systems Hardware. The equipment shall be examined to determine that it appears to be in good working order and has no "parts" that might be detrimental to the secure operation of the information system when placed under site control and cognizance. Subsequent changes and developments that affect security may require additional examination.

DRAFT

4. IDENTIFICATION AND AUTHENTICATION MANAGEMENT. Identification and authentication are required to ensure that users are associated with the proper security attributes, such as identity, protection level, or location. Controls, such as biometrics or smart cards, may be used at the discretion of the ISSO with approval of the ISSM and DAA.
- a. Identifier Management. User identifiers shall be managed in accordance with procedures identified in the SSP.
 - b. Authenticator Management. User authenticators shall be managed in accordance with procedures identified in the SSP.
 - c. Unique Identification. Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.
 - d. Authentication at Login. Users shall be required to authenticate their identities at “logon” time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user ID prior to the execution of any application or utility on the system.
 - e. Access to Authentication Data. Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.
 - f. User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the system.
 - g. User ID Removal. When, for example, an employee leaves the sponsoring organization or loses access for cause, that individual’s user ID and its authentication shall be removed or disabled from the system.
 - h. User ID Revalidation. The ISSO shall ensure that all active user IDs are revalidated at least annually, and information such as sponsor and means of offline contact (e.g., phone number, mailing address) is updated as necessary.
 - i. Protection of Authenticator. An authenticator that is in the form of knowledge or possession (password, smart card, keys) shall not be shared with anyone.
 - j. Protection of Passwords. When passwords are used as authenticators, the following shall apply.

DRAFT

- (1) Passwords shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.
 - (2) Passwords shall contain a minimum of six nonblank characters.
 - (3) Passwords shall be produced by a method approved by the DAA. In no case shall a user "supply" his/her own password. Password acceptability shall be based on the method of selection, the length of password, and the size of the password space. The password selection method, the length of the password, and the size of the password space shall be described in an attachment to the SSP.
 - (4) When an information system cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.
 - (5) User software including operating system and other security-relevant software comes with a few standard authenticators (e.g., SYSTEM, TEST, MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the information system. The ISSO shall also ensure that these passwords are changed after a new system release is installed or after other action is taken that might result in the restoration of these standard passwords.
 - (6) If the level of concern for confidentiality is low, the lifetime of a password shall not exceed 12 months. If the level of concern is medium or high, the lifetime of a password shall not exceed 6 months.
5. MAINTENANCE. Information systems are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified and unclassified information and facilities.
- a. Cleared Maintenance Personnel. Personnel who perform maintenance on systems shall be cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system. Cleared personnel who perform maintenance or diagnostics on information systems do not require an escort. However, when possible, an appropriately-cleared and technically-knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that the proper security and safety procedures are being followed.

DRAFT

b. Uncleared (or lower-cleared) Maintenance Personnel.

- (1) If appropriately-cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided a fully-cleared and technically-qualified escort monitors and records their activities in a maintenance log.
- (2) Uncleared maintenance personnel who are not U.S. citizens shall have Initiation and Termination performed by the fully-cleared and technically-qualified escort. In addition, keystroke monitoring shall be performed during their access to the system.
- (3) Prior to maintenance by uncleared personnel, the information system shall be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured. When a system cannot be cleared, ISSM-approved procedures shall be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive data that is contained on the system.
- (4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks or cassettes that are integral to the operating system, shall be used for all maintenance operations performed by uncleared personnel. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. Maintenance procedures for an information system using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis.

c. General Maintenance Requirements.

- (1) A maintenance log shall be maintained. The maintenance log shall include the date and time of maintenance, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts.
- (2) Maintenance of systems shall be performed on-site whenever possible. Equipment repaired off-site and intended for reintroduction into a facility may require protection from association with that particular facility or program.
- (3) If systems or system components are removed from the facility for repair, they shall first be purged and downgraded to an appropriate level, or sanitized of all

DRAFT

classified data and declassified in accordance with ISSM-approved procedures. The ISSO shall approve the release of all systems and all parts removed from the system.

- (4) Introduction of network analyzers (e.g., sniffers) that would allow maintenance personnel to do keystroke monitoring shall be approved by the ISSM prior to being introduced into an information system.
- (5) If maintenance personnel bring into a facility diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics), the media containing the programs shall be checked for malicious codes before the media is connected to the system. The media shall remain within the facility and shall be stored and controlled at the level of the information system. Prior to entering the facility, maintenance personnel shall be advised that they shall not be allowed to remove media from the facility. If deviation from this procedure is required under special circumstances, the following shall occur each time the diagnostic test media is introduced into a facility: the media shall undergo stringent integrity checks (e.g., virus scanning, checksum, etc.) prior to being used on the information system and, before leaving the facility, the media shall be checked to ensure that no classified information has been written on the media. Such a deviation shall be approved by the ISSM.
- (6) All diagnostic equipment and other devices carried into a facility by maintenance personnel shall be handled as follows.
 - (a) Systems and system components being brought into the facility shall be inspected for improper modification.
 - (b) Maintenance equipment capable of retaining information shall be appropriately sanitized by procedures outlined in periodic guidance issued by the ISPM before being released. If the equipment cannot be sanitized, the equipment shall remain within the facility, be destroyed, or be released under procedures approved by the DAA and the data owner(s) or responsible official(s).
 - (c) Replacement components may be brought into the facility for the purpose of swapping with facility components. However, any component placed into an information system shall remain in the facility until proper release procedures are completed. Any component that is not placed in an information system may be released from the facility.

DRAFT

- (d) Communication devices with transmit capability (e.g., pagers, RF LAN connections, etc.) belonging to the maintenance personnel or any data storage media not required for the maintenance visit shall remain outside the system facility for return to the maintenance personnel upon departure from the facility.
- (7) Maintenance changes that impact the security of the system shall receive a configuration management review.
- (8) After maintenance has been performed, the security features on the information systems shall be checked to ensure that they are still functioning properly.

d. Remote Maintenance.

- (1) Remote Diagnostic Maintenance service may be provided by a service or organization that **does** provide the same level and category(ies) of security. The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with national policies and procedures applicable to the sensitivity level of the data being transmitted.
- (2) If remote diagnostic or maintenance services are required from a service or organization that **does not** provide the same level of security required for the system being maintained, the information system shall be sanitized and in a stand-alone mode prior to the connection of the remote access line. If the system cannot be sanitized (e.g., due to a system crash), remote diagnostic and maintenance services shall not be allowed. Initiation and termination of the remote access shall be performed by the ISSO. Keystroke monitoring shall be performed on all remote diagnostic or maintenance services. A technically qualified person shall review the maintenance log to ensure the detection of unauthorized changes. The ISSO shall ensure that maintenance technicians responsible for performing remote diagnosis/maintenance are advised (contractually, verbally, by banner, etc.) prior to remote diagnostics/maintenance activities that keystroke monitoring shall be performed. Maintenance personnel accessing the information systems at the remote site shall be cleared to the highest level of information processed on that system prior to sanitization. Installation and use of remote diagnostic links shall be addressed in the SSP. An audit log of all remote maintenance, diagnostic, and service transactions shall be maintained and periodically reviewed by the ISSO. Other techniques to consider include

DRAFT

encryption and decryption of diagnostic communications, strong identification and authentication techniques, such as tokens, and remote disconnect verification.

- (3) System maintenance requirements and vulnerabilities shall be addressed during all phases of the system life cycle. Specifically, contract negotiations shall consider the security implications of system maintenance.

6. MALICIOUS CODE.

- a. Site Policies. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented.
- b. Personal Software. The use of software purchased or developed by an individual for personal use on an information system is discouraged. If such software is required or desired to enhance the information system operation, each installation of the software shall be approved by the ISSM.
- c. Public Domain Software. The use of public domain software on an information system is strongly discouraged. Procedures shall be implemented to carefully examine this software for malicious code before it is introduced into the information system environment.
- d. Review of Security-Relevant Changes. All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation. All security-relevant modifications shall be subject to the provisions of the system configuration management program. The ISSM shall notify the DAA of requests for changes to the resources that deviate from the requirements of the approved SSP. The DAA shall consider the system for reaccreditation.

7. MARKING HARDWARE, OUTPUT, AND MEDIA. Markings on hardware, output, and media shall conform to guidelines issued by the ISPM. If the marking required by the guidelines is impractical or interferes with the operation of the media, the DAA may approve alternate marking procedures. The alternate marking procedures shall be documented.

- a. Hardware Components. Procedures shall be implemented to ensure that all components of an information system, including input/output devices, terminals, stand-alone microprocessors, or word processors used as terminals, bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the

DRAFT

information system. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the information system and displayed on the screen.

- b. Hard Copy Output. Hard copy output includes paper, fiche, film, and other printed media. The accreditation level of the accredited information system shall be marked on all hard copy output that is retained in, or distributed from, the facility unless an appropriate classification review has been conducted or the information has been output by a tested program verified to produce consistent results and approved by the DAA. Such programs will be tested on a statistical basis to ensure continuing performance. Once a review has been conducted by an authorized classifier, that matter must be marked in accordance with DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.
 - c. Removable Media. Procedures shall be implemented by the ISSO to ensure that personnel handling removable media apply visible, human-readable, external markings to the media. Removable media shall be marked with the accreditation level of the information system unless an appropriate classification review has been conducted, or the information on the media has been outputted by a tested program or methodology verified to produce consistent results and approved by the DAA.
 - d. Unclassified Media. In facilities where some of the information systems are operated as classified and some are dedicated to unclassified operation, the removable unclassified media shall be uniquely marked to protect from the mixing of the media.
8. PERSONNEL SECURITY. Personnel play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their information-processing systems. Personnel directly involved with a system may be users, operators, administrators, COMSEC custodians, and installers/maintainers. Duties, responsibilities, privileges, and specific limitations of information systems users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system.
- a. Access Approvals. Background investigations of applicants, employees, contractors, and other individuals shall be performed as necessary to meet appropriate standards; for access to classified information, the appropriate standards are national standards.
 - (1) For systems that process classified information at Protection Level 1, 2, or 3, individuals shall be **cleared** to the highest level of classification processed on that

DRAFT

system. For Protection Level 4, 5, or 6 systems, the individual need only to be **cleared** for the information to which they are allowed access.

- (2) For Protection Level 1, 2, or 3 systems, the individuals shall have all required formal access approval(s) for all information on the systems. For Protection Level 4, 5, or 6 systems, the individuals need formal access approval for only that information to which they are allowed access.

b. General Users.

- (1) General users shall:
 - (a) access only that data, control information, and software for which they are authorized access and have a need-to-know;
 - (b) immediately report all security incidents and potential threats and vulnerabilities involving information systems to the appropriate ISSO;
 - (c) protect their authenticators and report any compromise or suspected compromise of an authenticator to the appropriate ISSO;
 - (d) ensure that system media and system output is properly classified, marked, controlled, and stored;
 - (e) protect terminals from unauthorized access;
 - (f) inform the ISSO when access to a particular information system is no longer required (e.g., completion of project, transfer, retirement, resignation, etc.);
 - (g) observe rules and regulations governing the secure operation and authorized use of information systems;
 - (h) use the information system only for official government business.
- (2) General users shall not attempt to:
 - (a) introduce malicious code into any information system or physically damage the system;

DRAFT

- (b) bypass, strain, or test security mechanisms (If security mechanisms must be bypassed for any reason, users shall coordinate the procedure with the ISSO, and receive written permission from the ISSM for the procedure.);
 - (c) introduce or use unauthorized software, firmware, or hardware on an information system;
 - (d) assume the roles and privileges of others and attempt to gain access to information for which they have no authorization;
 - (e) relocate information system equipment without proper authorization.
- c. Privileged Users.
- (1) The number of privileged users shall be limited to the absolute minimum number needed to manage the system.
 - (2) Examples of privileged users (for multi-user systems) include:
 - (a) users having “super-user,” “root,” or equivalent access to a system (i.e., system administrators, computer operators, perhaps system security officers, etc.); includes those individuals who have near or complete control of the operating system of the machine or information system or who set up and administer user accounts, authenticators, and the like;
 - (b) users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexors, and other key information system equipment;
 - (c) users who have been given the power to control and change other users’ access to data or program files (i.e., applications software administrators, administrators of specialty file systems, database managers, etc.);
 - (d) users who have been given special access for troubleshooting information systems/security monitoring functions (i.e., those using information system analyzers, management tools, etc.).
 - (3) All privileged users shall be responsible for all the requirements as stated for general users.

DRAFT

(4) Privileged users shall:

- (a) be U.S. citizens unless otherwise approved in writing by the DAA;
- (b) possess access approvals to all the information on the system;
- (c) possess clearance equal to the highest classification of data processed on or maintained by the information system;
- (d) protect the root or superuser authenticator at the highest level of data it secures and not share the authenticator and/or account;
- (e) be responsible for all superuser or root actions under his/her account;
- (f) report any and all information system problems to the ISSO;
- (g) use special access or privileges granted only to perform authorized tasks and functions.

(5) Privileged users shall not:

- (a) enroll any unauthorized user on an information system;
- (b) use special access or privileges to perform unauthorized tasks or functions.

9. PHYSICAL SECURITY.

- a. Protection. The information and system shall be located in an area appropriate to the classification and sensitivity of the data.
- b. Visual Access. Devices that display or output information in human-readable form shall be positioned to deter unauthorized individuals from reading the information without the knowledge of the user.
- c. Information Protection. Information shall be protected in accordance with DOE Manual 5632.1C-1, Chapter III.
- d. Unescorted Access. All personnel granted unescorted physical access to the system or information shall have a need-to-know for all information in the area or on the information system.

DRAFT

10. PROTECTION OF MEDIA.

- a. Media Protection. Media must be protected by at least one (or a combination) of the following until the media has been reviewed following a DAA or DAA-approved procedure:
 - (1) storage in an area approved for open storage of information at the accreditation level of the information system; or
 - (2) storage in an area approved for open storage of information at the accreditation level of the information system while continuously attended, if the area is continuously attended; or
 - (3) Type 1 encryption of stored data; or
 - (4) GSA-Approved Container.
- b. Removable Media. Removable media shall be controlled and protected in a manner similar to that used for classified paper materials.
- c. Laser Printers.
 - (1) Property Protection Area. If the laser printer is located in a property protection area approved for classified processing, the toner cartridge shall be sanitized at the end of the session using DAA-approved procedures, or the toner cartridge shall be removed from the printer and stored in a container approved for the storage of classified matter.
 - (2) Limited/Exclusion Area. If the laser printer is located in a limited area, the toner cartridge is protected while it is in the printer. If the toner cartridge must be removed from the printer, the toner cartridge shall be stored in a container approved for the storage of information on the system, or the toner cartridge shall be sanitized using DAA-approved procedures.

11. REVIEW OF OUTPUT.

- a. Human-readable Output Review. An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the system boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

DRAFT

- b. Media Review. Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. Random or representative sampling techniques may be used to verify the proper marking of large volumes of output. The media sampling procedures shall be defined and documented. DAA-approved automated techniques may be used to verify the proper marking of output.

CHAPTER X

PROTECTION REQUIREMENTS

1. INTRODUCTION. Each section of this chapter describes the implementation requirements for a different protection measure.
2. ALTERNATIVE POWER SOURCE. An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An alternate power source can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.
 - APS-1 Requirements.
 - a. Alternative Power Source. The decision not to use an alternative source of power, such as an uninterruptible power supply (UPS) for the system, shall be documented.
 - APS-2 Requirements. Instead of APS-1:
 - b. Alternative Power Source. Procedures for the graceful shutdown of the system shall ensure no loss of data.
 - APS-3 Requirements. Instead of APS-2:
 - c. Alternative Power Source. Procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.
 - Profile Requirements.

Requirements			
Availability	Low	Medium	High
Alternative Power Source	APS-1	APS-2	APS-3

DRAFT

3. AUDIT CAPABILITY. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user was responsible for them.

- AUD-1 Requirements.

- a. Audit Trail Creation. The system shall automatically create and maintain an audit trail or log that includes records of **successful and unsuccessful logons and logoffs**.

For each recorded event, the audit record shall contain, at a minimum, the date and time of event, the user ID, the type of event, and the success or failure of the event.

- b. Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.
 - c. Audit Trail Analysis. Audit analysis and reporting shall be scheduled, performed, and documented on a regular basis. The frequency of the review shall be documented in an attachment to the SSP.
 - d. Audit Record Retention. Audit records shall be retained for at least 6 months.
 - e. Alternative Methods. If it is not possible to provide an automated audit trail or log, an alternative method of accountability for user activities on the system shall be developed and documented.
- AUD-2 Requirements. In addition to AUD-1:
- f. Audit Trail Creation. In addition to the audit trail creation requirement in AUD-1, the system shall automatically create and maintain an audit trail that includes records of:
 - privileged activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users;
 - successful and unsuccessful accesses to security-relevant files, including creation, open, close, modification, and deletes;
 - starting and ending times of each access to the system;
 - changes in user authenticators;

DRAFT

- the blocking or blacklisting of a user ID, terminal, or access port and the reason for the action;
- denial of access resulting from an excessive number of unsuccessful logon attempts.

For each recorded event, the audit record shall contain, at a minimum, the date and time of event, the user ID, the type of event, and the success or failure of the event.

- g. Audit Failure. Procedures shall be implemented to ensure alternate audit capability or system shutdown in the event of audit failure.

- AUD-3 Requirements. In addition to AUD-2:

- h. Automated Audit Analysis. Audit analysis and reporting using automated tools shall be scheduled and performed.

- i. Security Label Changes. The system shall automatically record the creation, deletion, or changes in security labels.

- AUD-4 Requirements. In addition to AUD-3:

- j. Continuous Monitoring. Auditing shall include the continuous, online monitoring of auditable events. The system shall notify an authorized person when imminent violations of security policies are detected.

- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Audit Capability	AUD-1	AUD-1	AUD-2	AUD-3	AUD-4	AUD-4

Requirements			
Integrity	Low	Medium	High
Audit Capability	AUD-1	AUD-2	AUD-4

DRAFT

4. **BACKUP AND RESTORATION OF DATA.** The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

- **BRD-1 Requirements.**
 - a. **Backup Procedures.** Procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation, shall be documented.
 - b. **Backup Frequency.** The frequency of backups shall be defined by the ISSO, with the assistance of the data owner(s), and documented in the backup procedures.
- **BRD-2 Requirements.** In addition to BRD-1:
 - c. **Backup Media Storage.** Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or offsite, so as to reduce the possibility that a common occurrence could eliminate the on-site backup data and the off-site backup data.
 - d. **Verification of Backup Procedures.** Backup procedures shall be periodically verified by confirming that the date of last backup is consistent with the backup procedures.
- **BRD-3 Requirements.** In addition to BRD-2:
 - e. **Information Restoration Testing.** Complete restoration of information from backup media shall be tested on a periodic basis. The frequency of restoration testing shall be defined and documented in the backup procedures.
- **Profile Requirements.**

Requirements			
Availability	Low	Medium	High
Backup and Restoration of Data	BRD-1	BRD-2	BRD-3

DRAFT

5. CHANGES TO DATA. The control of changes to data includes the deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

- CD-1 Requirements.

- a. Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data are executed only by authorized personnel or processes.

- CD-2 Requirements. In addition to CD-1:

- b. Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of unauthorized data changes and the off-line verification of all changes at all times.

- Profile Requirements.

Requirements			
Integrity	Low	Medium	High
Changes to Data	CD-1	CD-1	CD-2

6. COMMUNICATIONS. Information protection is required whenever National Defense information (classified or any of the special categories of unclassified information under the security cognizance of NN) is to be transmitted or carried to, or through, areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

- COM-1 Requirements.

- a. Protections. One or more of the following protections shall be used:

- (1) information distributed only within an area approved for open storage of the information, or
- (2) NSA-approved encryption mechanisms appropriate for the encryption of classified information, or

DRAFT

- (3) NIST-approved encryption mechanisms appropriate for the encryption of unclassified information, or
- (4) Protected Distribution System, or
- (5) trusted courier.

- COM-2 Requirements. In addition to COM-1:

- b. Public Switched Networks. Any classified system connected to a public switched network (e.g., Internet) or an internal network that is not accredited at the same level must utilize a Controlled Interface (CI) that meets the requirements in Chapter VI and performs the following.

- (1) Review Before Release. Unclassified communication from the inside shall be reviewed for classification before being released.
 - (2) Encryption of Message Body. The body of classified communication from the inside shall be encrypted with NSA-approved encryption mechanisms appropriate for the classification of the information for encryption of stored data.
 - (3) Notification of Recipient. Communication from the outside must have an inside sponsor (i.e., the CI will notify the sponsor of the communication and release the communication on notification from the sponsor).
 - (4) Review of Outside Communications. Communication from the outside shall be reviewed for viruses and other malicious code.
 - (5) End-to-end Integrity. Integrity attributes adequate to ensure the end-to-end integrity of transmitted information (including labels and security parameters) shall be included with all information transmitted externally to a system or network.
- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Communications	COM-1	COM-1	COM-1	COM-2	COM-1	COM-1

DRAFT

NOTE: The Department of Energy will not approve systems at Protection Level 5 or Protection Level 6 to be attached to public switched networks.

Requirements			
Integrity	Low	Medium	High
Communications	COM-1	COM-1	COM-2

7. CONFIGURATION MANAGEMENT. Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
- CM-1 Requirements.
 - a. Configuration Documentation. Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location.
 - b. System Connectivity. Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.
 - CM-2 Requirements. In addition to CM-1:
 - c. Connection Sensitivity. The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.
 - d. CM Plan. The CM plan shall be documented and shall include:
 - (1) formal change control procedures for security-relevant hardware and software;
 - (2) procedures for management of all documentation, such as the Systems Security Plan (SSP) and security test plans, used to ensure system security;
 - (3) workable processes to implement, periodically test, and verify the plan.

DRAFT

- CM-3 Requirements. In addition to CM-2:
- e. CM Plan. In addition to the requirements of the CM plan in CM-2, the CM plan shall include:
- (1) a CM control board that implements procedures to ensure the security review and approval of changes that affect the SSS and
 - (2) a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.
- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Configuration Management	CM-1	CM-1	CM-1	CM-2	CM-3	CM-3

Requirements			
Integrity	Low	Medium	High
Configuration Management	CM-1	CM-2	CM-3

8. DISASTER RECOVERY PLANNING.

- DRP-1 Requirements.
- a. Mission Essential. The site's Mission-Essential Applications and Development of Descriptions of Each Mission Essential Application shall be identified.
 - b. Plan Decision. A decision concerning the need for a continuity of operations plan or contingency plan for each information system shall be made by the manager or supervisor directly responsible for the system. This decision shall be documented and signed by the manager or supervisor. A statement of the decision and the basis for that decision shall be documented in the SSP. If a continuity of operations plan or contingency plan is not needed, a statement to that effect shall be included in the SSP.

DRAFT

- c. Procedures. Documented procedures for the backup of all essential information, software, and documentation on a regular basis shall be implemented. The backup procedures shall be attached to or referenced in an attachment to the SSP. The frequency of backups shall be defined by the ISSO, with the assistance of the data owner(s), and documented in the backup procedures.
- d. Plan Elements. The elements of a disaster recovery plan defined in MA-365, "Disaster Recovery Program Guideline," dated 7-91, shall be addressed in the plan(s).
 - DRP-2 Requirements. In addition to DRP-1:
- e. Verification of Procedures. Backup procedures shall be periodically verified by confirming that the date of last backup is consistent with the backup procedures. The frequency of verification shall be defined by the ISSO, with the assistance of the data owner(s), and documented in the backup procedures.
 - DRP-3 Requirements. In addition to DRP-2:
- f. Testing of the Disaster Recovery Program. A testing plan shall be developed that addresses the criteria for evaluating the test results and the schedule for performing the tests.
 - Profile Requirements.

Requirements			
Availability	Low	Medium	High
Disaster Recovery Planning	DRP-1	DRP-2	DRP-3

9. INDEPENDENT VALIDATION AND VERIFICATION.

- IVV-1 Requirements.
- a. IV&V Team. An Independent Validation and Verification (IV&V) team, in coordination with the ISSM, shall:
 - (1) assist in the design phase of the system,

DRAFT

- (2) assist in determining and developing the certification test requirements,
 - (3) assist in the certification testing, and
 - (4) evaluate the security of the implemented system.
- b. IV&V Request. The request for an IV&V team shall be forwarded through the DAA to the ISPM by the ISSM. The request shall identify funding sources for the IV&V team.
- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Independent Validation and Verification					IVV-1	IVV-1

10. **RESOURCE ACCESS CONTROLS**. Information systems shall store and preserve the integrity of the sensitivity of all information internal to the information system.

- RAC-1 Requirements.
- a. Discretionary access controls shall be provided.
- RAC-2 Requirements. In addition to RAC-1:
- b. Security Labels. The information system shall place electronic security labels on all entities (e.g., files) reflecting the sensitivity (classification level, classification category, and handling caveats) of the information for resources and the authorizations (security clearances, need-to-know, formal access approvals) for users. These labels shall be an integral part of the electronic data or media and shall be compared to the user or resource profile and validated before a user or resource is granted access to the entity.
- c. Export of Security Labels. Security labels exported from the information system shall accurately represent the corresponding security labels on the information in the originating information system.
- d. Security Label Integrity. The information system shall ensure the following:

DRAFT

- (1) integrity of the security labels,
 - (2) the association of a security label with the transmitted data, and
 - (3) enforcement of the control features of the security labels.
- RAC-3 Requirements. In addition to RAC-2:
- e. Device Labels. The information system shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.
 - f. Mandatory Access Controls. Mandatory access controls shall be provided.
- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Resource Access Control		RAC-1	RAC-1	RAC-2	RAC-3	RAC-3

11. RESOURCE UTILIZATION.

- RU-1 Requirements.
- a. Resource Reallocation. The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.
- RU-2 Requirements. In addition to RU-1:
- b. Resource Allocation. The Security Support Structure shall provide the capability to control a defined set of system resources (e.g., memory, disk space) such that no one user can deny another user access to the resources.

- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Resource Utilization		RU-1	RU-1	RU-2	RU-2	RU-2

12. SESSION CONTROLS. Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user's session.

- SC-1 Requirements.
 - a. User Notification. All authorized information system users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user. The user shall be required to take positive action to remove the notice from the screen. Monitoring and recording, such as collection **and** analysis of audit trail information, shall be performed.

The following is a suggested warning text to the user.

“WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.”

If it is not possible to provide an “initial screen” warning notice, other methods of notification shall be developed and approved by the DAA.

- b. Successive Login Attempts. If the operating system provides the capability, successive logon attempts shall be controlled:
 - by denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID;

DRAFT

- by limiting the number of access attempts in a specified time period;
 - by the use of a time delay control system; or
 - by other such methods, subject to approval by the DAA.
- c. System Entry. The system shall grant system entry only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.
- SC-2 Requirements. In addition to SC-1:
- d. Multiple Login Control. If the information system supports multiple login sessions for each user identifier or account, the information system shall provide a protected capability to control the number of login sessions for each user identifier, account, or specific port of entry. The information system default shall be a single login session.
- e. User Inactivity. The information system shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSP.
- f. Logon Notification. If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.
- SC-3 Requirements. In addition to SC-2:
- g. Security Level Changes. The information system shall immediately notify the user of each change in the security level or compartment associated with that user during an interactive session. A user shall be able to query the information system as desired for a display of the user's complete sensitivity label.

- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Session Controls	SC-1	SC-2	SC-2	SC-3	SC-3	SC-3

13. SECURITY DOCUMENTATION. Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The Systems Security Plan is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a site or information contained in other documents may be attached to or referenced in the SSP.

- SD-1 Requirements.

- a. SSP. The SSP shall contain the following:

- (1) System Identification.

- (a) Security Personnel. The name, location, and phone number of the responsible system owner, DAA, ISSM, and ISSO.
- (b) Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

- (2) System Requirements Specification.

- (a) Sensitivity or Classification Levels of Information. The sensitivity or classification levels and categories of all information on the system.
- (b) Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

DRAFT

- (c) Variances from the Protection Profile Requirements. A description of any approved deviations from the protection profile. A copy of the approval documentation shall be attached to the SSP.
 - (3) System Specific Risks and Vulnerabilities. A description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the site or system, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities shall be described.
 - (4) System Configuration. A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems.
 - (5) Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the DAA responsible for this system. A copy of any memoranda of understanding with other agencies shall be attached to the SSP.
 - (6) Security Support Structure. A brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.
- b. Certification and Accreditation Documentation.
 - (1) Certification documentation. A certification statement that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the responsible system owner or the ISSO.
 - (2) Accreditation Documentation. Documentation for accreditation includes the certification statement and a cover letter including a recommendation for DAA approval or disapproval.

- SD-2 Requirements. In addition to SD-1:
- c. System Implementation of Requirements. A brief description of how the system implements each of the security requirements.
- SD-3 Requirements. In addition to SD-2:
- d. Certification and Accreditation Documentation.
 - (1) Security Testing. Test plans, procedures, and test reports.
 - (2) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the SSP.
 - (3) Compliance Statements. Statements of compliance that TEMPEST, PDS, and TSCM, and other security requirements have been met.
 - (4) IV&V Report. Report from the Independent Validation and Verification Team.
- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Security Documentation	SD-1	SD-1	SD-2	SD-2	SD-3	SD-3

14. SEPARATION OF FUNCTIONS.

- SF-1 Requirements.
- a. Separation of Functions. The functions of the ISSO and the system manager shall not be performed by the same person.

DRAFT

- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Separation of Functions				SF-1	SF-1	SF-1

15. **SYSTEM RECOVERY.** System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.

- SR-1 Requirements.

- a. Controlled Recovery. Procedures and information system features shall be implemented to ensure that information system recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the information system shall be accessible only via terminals monitored by the ISSO or his/her designee, or via the information system console.

- SR-2 Requirements.

- b. Trusted Recovery. Procedures and technical system features shall be implemented to ensure that system recovery is done in a trusted and secure manner. Procedures to mitigate all information system recovery circumstances where the restoration of protection features cannot be ensured shall be implemented and documented in an attachment to the SSP.

- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
System Recovery	SR-1	SR-1	SR-1	SR-1	SR-2	SR-2

16. **SECURITY SUPPORT STRUCTURE.** Those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system.

DRAFT

- SSS-1 Requirements.
 - a. Access to Protection Functions. Access to hardware/software/firmware that perform systems or security functions shall be limited to authorized personnel.
- SSS-2 Requirements. In addition to SSS-1:
 - b. SSS Protection Documentation. The protections and provisions of the SSS shall be documented.
 - c. Informal Description of Policy Model. An informal description of the security policy model enforced by the SSS shall be documented.
 - d. Periodic Validation of SSS. Features and procedures shall exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS.
- SSS-3 Requirements. In addition to SSS-2:
 - e. SSS Isolation. The SSS shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures).
 - f. Policy Description. A description of the security policy model enforced by the SSS shall be documented with an explanation that shows it is sufficient to enforce the security policy. All interfaces to the SSS shall be included in the explanation.
- Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Security Support Structure	SSS-1	SSS-1	SSS-1	SSS-2	SSS-3	SSS-3

Requirements			
Integrity	Low	Medium	High
Security Support Structure	SSS-1	SSS-2	SSS-3

DRAFT

Requirements			
Availability	Low	Medium	High
Security Support Structure	SSS-1	SSS-2	SSS-3

17. **SECURITY TESTING.** Ongoing security testing is the verification of correct operation of the protection measures in a system.

- **ST-1 Requirements.**
 - a. **Verification of Functions.** The security functions (e.g., audit trails, system passwords) defined in the PP shall be verified prior to certification by performing tests to confirm correct operation of all security-relevant functions when activated with normal input values.
- **ST-2 Requirements.** In addition to ST-1:
 - b. **Certification Testing.** Certification testing shall include the security function verification tests, tests to verify that the security functions do not have any undesired effect(s) on the information system, and tests to verify that the security functions perform correctly when activated with abnormal input values.
 - c. **Ongoing Testing.** Ongoing security performance testing of the system shall be conducted regularly to ensure that the security features continue to function correctly. The ongoing security performance tests may include all or parts of the security function verification and certification tests. The methods for determining that these features continue to be implemented during the life cycle of the information system (e.g., after system updates) shall be documented.
- **ST-3 Requirements.** In addition to ST-2:
 - d. **Certification Test Reporting.** Certification testing provides assurance that the information system is operating in accordance with the approved SSP. The certification test results, when satisfactory, provide the DAA with supporting documentation for the accreditation of the information system.
 - (1) **Certification Test Plans.** The ISSO shall develop the certification test plan to ensure that the information system has been implemented and is operating in

DRAFT

accordance with the SSP. The certification test plan shall be approved by the DAA. If the security features of the information system, as specified in the SSP, are expected to restrict user access, for example, these features shall be tested to ensure that they are implementing the specified security requirements.

- (2) Certification Test Performance. The ISSO shall ensure that the specified tests are performed.
 - (3) Documentation. The results of certification tests and an analysis of the results shall be documented.
 - (4) Additional Tests. Following receipt of the certification documentation, the DAA may designate additional tests that shall be performed prior to meeting accreditation requirements.
- ST-4 Requirements. In addition to ST-3:
 - e. Penetration Testing. Ongoing prudent penetration testing shall be performed to identify major or obvious vulnerabilities in the system. The test methodology and procedures shall be described in a security test plan. The ongoing penetration tests may include all or parts of the security function verification tests.
 - f. Independent Validation and Verification. An Independent Validation and Verification team shall assist in the certification testing of an information system and shall perform validation testing of the system as required by the DAA.
 - Profile Requirements.

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Security Testing	ST-1	ST-2	ST-2	ST-3	ST-4	ST-4

Requirements			
Integrity	Low	Medium	High
Security Testing	ST-1	ST-3	ST-4

DRAFT

18. **TRUSTED PATH.** Users often need to perform functions, such as authentication, through direct interaction with the SSS. A trusted path ensures that the user is communicating directly with the SSS. Trusted path exchanges may be initiated by a user or the SSS. A user response via the trusted path guarantees that untrusted processes cannot intercept or modify the user's response.

- **TP-1 Requirements.**

- a. **Authentication Path.** The information system shall support a trusted path between itself and the user for initial identification and authentication.

- **Profile Requirements.**

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Trusted Path					TP-1	TP-1

ATTACHMENT 1

DEFINITIONS

Accreditation - The formal acknowledgment (written or electronic) of the decision by the designated approval authority to authorize an information system to process, store, transfer, or provide access to information in a specific information systems security environment established by a specific SSP.

Availability - The attribute of information being in the place, at the time, and in the form needed by the user. Denotes the goal of ensuring that information and information processing resources both remain readily accessible to their authorized users.

Boundary - The conceptual limit of an information system that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.

Classified Information Systems Security Program Manager (ISPM) - The individual responsible for the development of Departmental policies, standards, guidelines, and procedures for the protection of classified information in automated information systems.

Classified Information Systems Security Operations Manager (ISOM) - The technical expert responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an information system.

Classified Information Systems Security Site Manager (ISSM) - The manager responsible for a site information systems security program.

Classified Information Systems Security Officer (ISSO) - The person responsible for ensuring that protection measures are installed and operational security is maintained for one or more specific information system.

Clearing - Removal of data from an information system, its storage media, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (i.e., through the keyboard). NOTE: Clearing does not permit the reuse of media at a lower classification level or unclassified if the media has contained classified information.

Confidentiality - The critical attribute of information of being inaccessible except to persons or processes that have an authorization and a legitimate need or right to read that information.

DRAFT

Data Steward - The individual responsible for introducing and managing information on an information system. This person is the “steward” of the information and is responsible for its generation, management, and destruction.

Data Owner - The person who declares the sensitivity, classification, category, and dissemination requirements of the information. The person to whom the data belongs.

Designated Approval Authority - The official with the authority to formally grant approval for operating an information system; the person who determines the acceptability of the remaining or residual risk in a system that is prepared to process classified information and either accredits or denies operation of the system for the Department.

Information System - As defined in *NSTISSC 4009, National Information Systems Security (INFOSEC) Glossary*, dated 5 June 1992, “any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.”
NOTE: COMSEC and TSCM Requirements are contained in other Orders.

Integrity - The attribute of information of being a true, complete representation of its original content, even when undergoing changes in form or storage medium.

Level of Concern - An expression of the information’s perceived value and the consequences of loss of integrity, availability, or confidentiality.

Perimeter - All those components of the system that are to be accredited. NOTE: As a rule, separately accredited components are not included within the perimeter, but those components are within the boundary.

Protection Level -

Residual Risk - The remaining risk of operating the system after application of mitigating factors.
NOTE: Such mitigating factors often include, but are not limited to:

- minimizing initial risk by selecting a system known to have fewer vulnerabilities;
- reducing vulnerabilities by implementing countermeasures;
- reducing consequence by limiting the amounts and kinds of information on the system; and

DRAFT

- using classification and compartmentation to lessen threat by limiting the adversaries' knowledge of the system.

Sanitization - The removal of information from media or equipment such that data recovery using any known technique or analysis is prevented. NOTE: Sanitizing shall include the removal of data from the media, as well as the removal of all sensitivity or classified labels, markings, and activity logs.

Site Manager - The director or manager of a site; the person who is responsible for management of all activities at a site.

Special categories of unclassified information under the security cognizance of NN - UCNI, NNPI, EXPORT/IMPORT, and OOU as it relates to National Security Interests of the Department/Government to include information on Critical Infrastructure that could increase the risk to our critical resources.

User - An individual who can receive information from, input information to, or modify information on, a system without an independent human review. In a processing context, this also includes a process acting on behalf of a user. NOTE: It is often convenient to refer to a user who is **NOT** a privileged user as a General User.

Direct User - A user who has physical or electronic access to any component of the system.

Indirect User - A user who has access to information from the system without an independent human review, but who does not have physical or electronic access to the system itself.

Privileged User - A user who has access to system control, monitoring, or administration functions (e.g., system administrator, system security officer, maintainers, system programmers, etc.).

DRAFT